INFORMATION ASSURANCE EVENT/INCIDENT CHECKLIST

For use of this form, see AR 25-1

INSTRUCTIONS. ANSWER ALL QUESTIONS.
If a question does not apply, indicate N/A in the blank. Continue on reverse if necessary, and key to Section/Item No. below.

SECTION I. TARGET INFORMATION

1. Security Classification (Classified or Unclassified):

2. IP address of the targeted system(s) IP: Port:

3. MAC address of system NIC:

4. Serial number of system:

5. Machine name of the targeted system:

6. OS of the targeted system: Version:

7. How long has the system been on the network (since last reboot)?

8. Date and/or level of latest patch (from the event log):

9. System Hardware (i.e., SUN/COMPAQ/DELL):

10. Is the system a server? If YES, complete 10a-c below; if NO, go to Item 11.

a. Is system a web server?

b. Is the server publicly accessible?

c. Is system a network server?

11. List all other software installed on the system annotating authorized/unauthorized (list on reverse or attach separately).

12. What AV product is installed on the system: Version:

13. What was the latest AV update:

14. Were there any alerts from the AV product? If YES, identify them:

15. Accreditation date:

16. Is there an approved login warning banner?

17. When was intrusion/event detected?

18. Who discovered the intrusion/event?

19. How was intrusion/event detected? What suspicious activity caused or preceded the investigation?

20. What actions have the system administrator/security specialist taken in this incident to date?

21. If appropriate, has the site been blocked?

22. How was the intruder able to access the system?

23. Has the system adminstrator changed local administrator password for other related systems since the event (include date)?

24. Were files uploaded to the target system? List if info is available:

25. Physical location of the system:

26. Are there firewall/IDS logs available for this system? (DOIM will attach as appropriate)

SECTION II. IMPACT

1. No. manhours/people involved in investigation:

2. No. manhours/people involved in recovery:

3. No. manhours/people involved in lost productivity:

4. Any suspicious emails sent from the users account? If so, what were the destination addresses?

POC'S NAME: (Print) E-MAIL ADDRESS: PHONE:

POC'S SIGNATURE: DATE SIGNED:

UNIT COMMANDER'S NAME: (Print) E-MAIL ADDRESS: PHONE:

CONTINUATION: (Key to Section/Item No. on previous page)